CLAIMS

1. Process to manage data stored in a first memory of a first chip of a first chip card in which:

a first management code is produced with a first cryptographic algorithm based on a mother key and a first set of identification data of the first chip card,

this first management code is recorded in the first memory,

the first card is linked to a chip card reader, and

editing of data stored in the first memory is authorized if a secret code presented to the reader is compatible with the first management code recorded,

wherein the following steps are performed:

a second management code is produced with a second cryptographic algorithm based on data relating to the first card and a second set of identification data of a second chip card,

these data relating to the first card and the second management code are recorded in a second memory of a second chip of the second chip card, and

editing of the data stored in the second memory is authorized if a secret code presented to the reader is compatible with the second management code recorded.

2. The process according to claim 1 wherein the first and second management codes are secret codes.

3. The process according to claim 1 wherein the second algorithm is implemented in the chip of the card.

4. The process according to claim 1 wherein the first cryptographic algorithm is different from the second cryptographic algorithm, and the second cryptographic algorithm is symmetric.

5. The process according to claim 1, wherein the first cryptographic algorithm is the same as the second cryptographic algorithm.

6. The process according to claim 1, wherein the data relating to the first card is the first set of identification data of the first card or the first chip.

7. The process according to claim 1, the data relating to the first card is the first management code of the first card or the first chip.

8. The process according to claim 1 wherein a management code word is produced in the reader on the basis of the data relating to the first card, and a determination is made whether the card is authentic if this second management code word is compatible with a secret word.

9. The process according to claim 1 wherein a transmission attribute is associated with the data stored in the first memory, editing of these data is authorized so that they can be copied into the second memory depending on the value of this attribute, these data and this attribute are copied into the second memory, and this attribute gives information about a need to produce a second secret code when copying the data.

10. The process according to claim 9 wherein, in order to authorize editing of data contained in the first memory only under the control of a master system, a transmission attribute which gives information about a need for this

control by a master system is associated, this attribute is read prior to editing, and an editing program is started if the attribute having been read allows this.

11. The process according to claim 9 wherein the transmission attribute inhibits editing with a view to the data concerned being copied.

12. The process according to claim 9 wherein the data is copied into the memory in delayed time.

13. The process according to claim 1, wherein the card is a multi-application card, the data being associated with respective management codes.